G7 SECURITY MINISTERS' COMMITMENTS PAPER

Preamble

G7 countries continue to face complex challenges, ranging from terrorism and violent extremism to trafficking in persons. These issues threaten international peace and security and increase the vulnerability of our citizens, with disproportionate effects on women and girls.

Concerted action is required to address these issues. As such, we, the G7 Security Ministers and Members of the European Union, met to develop concrete approaches to strengthen security, protect our core democratic values, and work towards building a more peaceful and secure world.

We commit to working together to strengthen the fight against terrorism, address violent extremism, including its use of the internet, tackle threats to cyber security, and combat trafficking in persons.

Recognizing the importance of gender equality and women's empowerment, we worked closely with Canada's Gender Equality Advisory Council to help guide the integration of gender considerations throughout our commitments. We commit to ensuring approaches to these complex issues include meaningful participation of women in decision-making, and consider the impact on vulnerable populations as well as marginalized groups.

We reaffirm our commitment to fully implementing the Taormina Leaders' statement on the fight against terrorism and violent extremism and the Ischia joint communiqué, building on the Ise-Shima Action Plan.

1. Managing Threats Domestically

We continue to face a number of complex and multifaceted threats to our security, requiring domestic tools as well as effective multilateral cooperation to manage them. Increasingly our public security mission is dependent on the efficient and effective collection, analysis, sharing and understanding of information, within existing legal frameworks and consistent with privacy and human rights obligations. To this end, we intend to take measures to address barriers to information-sharing. We also continue to face other ongoing challenges including using intelligence as evidence, understanding the role of emerging technology and how it is exploited by adversaries, protecting public spaces that may be vulnerable to attacks, also known as soft targets, and threats posed by low sophistication tactics. We remain relentless in the fight against terrorism and to this end we will:

1.1 Implement United Nations Security Council Resolution 2396 (2017) with an emphasis on all of its provisions with respect to information sharing and in accordance with applicable domestic and international laws and regulations. The implementation includes the use of Advance Passenger Information (API) and Passenger Name Record (PNR), while respecting privacy rights and the protection of personal data information, biometrics, and watchlists in traveller screening.

1.2 Work closely together to identify emerging threat patterns and innovating capacities (including Chemical Biological Radiological and Nuclear related threats, explosive precursors), and low technology terrorist *modi operandi*, to effectively address the evolution of the threat.

1.3 Adopt proven platforms for the exchange of personal information to identify criminal and national security threats while facilitating legitimate movement, including, at the global level, those created through Interpol and, bilaterally, biometric-based, automated information sharing.

1.4 Explore solutions within existing legal frameworks to the challenges related to using intelligence, in particular, information collected from the battlefield, as evidence in the prosecution of terrorism-related offences.

1.5 Explore the role of emerging technologies, their exploitation by violent extremists, and the challenges and opportunities their adoption poses with regard to counterterrorism, counter-terrorist financing, and law enforcement efforts.

1.6 Examine ongoing challenges to protecting public spaces that may be vulnerable to attacks, commonly referred to as soft targets, and determine how best to mitigate risks associated with these targets. In addition, we will commit to analyzing how soft targets are used by domestic and transnational criminal actors, including through the collection of disaggregated data.

1.7 Commit to sharing best practices, including those developed through the Global Counter-Terrorism Forum (GCTF) on public messaging and awareness strategies to promote the protection of public spaces, involving relevant partners.

We will also encourage the Roma-Lyon Group on Transnational Organized Crime and Terrorism to:

1.8 Develop a G7 action plan on the protection of public spaces and ensure its monitoring.

1.9 Continue to work collaboratively to examine how to integrate gender considerations into the development, implementation, and evaluation of counterterrorism efforts, including by compiling and analyzing more research and data collection initiatives in relation to gender and counterterrorism.

2. Countering Violent Extremism

We will continue to support a whole-of society-approach to countering violent extremism and radicalization to violence, one that focuses on early prevention, supporting local level organizations and addressing community needs. To this end we will:

2.1 Work with existing multilateral research fora to develop a robust research network to facilitate the sharing of promising and best practices on approaches to prevention, intervention, and the reduction of harmful impacts on individuals, families, and communities, while avoiding stigmatization, including research aimed at understanding target groups as well as identifying places and factors likely to cultivate risks of radicalization to violence.

2.2 Share best and promising practices on effective intervention tools that are based on human rights and the rule of law and non-stigmatization, with an emphasis on gender-informed tools and those related to managing individuals with high levels of risk, need and vulnerability, and the prevention of radicalization to violence of offenders in detention facilities.

2.3 Work with civil society, including youth, faith-based organizations, women's organizations and community groups, to assist in identifying local needs to build resilience to violent extremist ideologies, such as human rights based education, training in critical thinking, and digital literacy. We will continue to work with civil society to engage in inclusive dialogue to address grievances as they arise.

2.4 Ensure continued efforts at the global level to counter violent extremism, in the context of the upcoming UN Global Counter-Terrorism Strategy Review and High Level Conference of Heads of Counter Terrorism Agencies and cooperate with the Global Counterterrorism Forum.

2.5 Support and coordinate capacity building in third countries to develop and advance initiatives to counter terrorism and violent extremism.

We will also encourage the Roma-Lyon Group on Transnational Organized Crime and Terrorism to:

2.6 Exchange ideas with a view to develop an action plan to detect, prevent and counter violent extremism, including gender-related analysis to enhance intervention strategies. This could include sharing information on capacity building initiatives in third countries.

3. Preventing Violent Extremist and Terrorist Use of the Internet

Violent extremist and terrorist organizations continue to exploit the internet and social media in a variety of ways, including through the production and dissemination of content that incites violence and hatred, and which is used for recruitment, facilitation, training, and financing purposes. We recognize that this exploitation and use of the internet reflects poorly on industry, can damage companies' reputations, and can lead to economic loses.

We will combat the exploitation of the internet and social media by violent extremists and terrorists, particularly Daesh and al-Qaida, and right and left wing violent extremists, by reinforcing collaboration with the Global Internet Forum to Counter Terrorism (GIFCT), the European Union (EU) Internet Forum, governments, researchers, academics and civil society. Building on the Ischia Joint Communiqué, we will:

3.1 Recognize the advancement GIFCT has made, continue to support its efforts, and call on GIFCT to:

3.1.1 Improve communication and transparency with our governments on industry-led efforts through its Executive Board, supported by a Secretariat;

3.1.2 Strengthen transparency and demonstrate progress against terrorist content online through the adoption of performance metrics consistent with those used by the EU Internet Forum on preventing and countering misuse of their platforms, including the removal of content and accounts within 1 hour of upload, where technically feasible, without compromising accuracy, and while respecting human rights and fundamental freedoms;

3.1.3 Explore methods of preserving removed violent extremist and terrorist content, and making it available upon request for investigation, prosecution, and accountability purposes;

3.1.4 Collaborate and include relevant partners, such as industry, government, academia, law enforcement and civil society as part of a collective approach to violent extremist and terrorist use of the internet;

3.1.5 Continue to develop, repurpose, and leverage and facilitate the sharing of technology and automated solutions for the rapid detection and removal of violent extremist and terrorist content within 1 hour of upload, where technically feasible, without compromising accuracy, and while respecting human rights and fundamental freedoms, taking into consideration gender disparities, and preserving evidence for law enforcement when necessary;

3.1.6 Prevent the recurrence of violent extremist and terrorist content by contributing to and utilizing the Shared Industry Hash Database and by publishing performance metrics;

3.1.7 Improve cooperation between the industry and internet referral units to expedite the treatment of referrals submitted by national authorities;

3.1.8 Support smaller platforms which are particularly vulnerable due to their limited resources to identify and remove violent extremist and terrorist material through the expansion of GIFCT membership; and,

3.1.9 Continue to provide and enhance its leadership by forming a collective industry wide voice.

3.2 Encourage industry to update the Terms of Service of all platforms so as to inform users of the consequences under the applicable national law of promoting terrorist content and using the crowdfunding and payment services provided online for terrorism financing.

3.2.1 Emphasize the need to support, local and credible gender-responsive voices, with a particular emphasis on youth, in the delivery and development of alternative and counter narratives.

3.2.2 Support well-informed and impactful research through free access to GIFCT's relevant findings and Application Programming Interfaces (APIs) to advance research in partnership with

GIFCT and its member companies. Efforts should be taken to ensure that data shared with researchers and academics is anonymized, disaggregated, and free of personally identifiable information, and used only for the intended research project.

3.2.3 We are fully supportive of the efforts of GIFCT to make a significant impact on the timely removal of terrorist content. We are closely assessing progress to determine if it is sufficiently made, on which basis some members may choose to explore options to incentivize further progress.

4. Cyber security and the fight against cybercrime

The growth and evolution of cyber capabilities have been matched by an increased number of risks in cyberspace, including the use of cyber capabilities for criminal purposes and attacks to critical infrastructure. As a result, countries are facing challenges in the development of legal and operational tools to respond to cyber risks.

We will pursue a collective approach to increase stability and security in cyberspace, and work together to improve our systemic risk management and measures to address the challenges along the cyber security continuum, including cybercrime. To this end we will:

4.1 Develop a common understanding of and share best practices for managing cyber risks to critical infrastructure at the national level.

4.2 Strengthen collective resolve to deter malicious cyber actors by imposing costs in a timely manner. The G7 members should attribute malicious behaviour when appropriate and jointly take action when it occurs.

4.3 Explore the creation of a link between all G7 cyber centres to: strengthen our resilience; better anticipate threats; and, explore options for possible collective responses.

4.4 Increase information sharing on the legal and operational tools each country is using to combat cybercrime from a law enforcement perspective.

4.5 Continue to support and promote the Budapest Convention on Cybercrime and strengthen efforts to attract additional States to join.

5. Trafficking in Persons

Women and girls account for the majority of trafficking victims worldwide. Trafficking in persons refers to a variety of types of exploitation including sexual exploitation, forced labour, slavery, servitude or the removal of organs (as defined by the Trafficking in Persons Protocol).We need to ensure our response is gender-sensitive and grounded in respect for human rights. In addition, our approach must recognize that marginalized groups, including indigenous women and girls, persons with disabilities, and the LGBTQI community, and migrants are more vulnerable to being trafficked. To this end we will:

5.1 Work with business and civil society to eliminate trafficking in persons, forced labour, child labour and all forms of slavery, including modern slavery, from G7 economies, by developing legislative, regulatory or policy frameworks, as appropriate.

5.2 Strengthen procurement practices to eliminate trafficking in persons, forced labour, child labour and slavery from global supply chains and work to build a culture of consumer awareness.

5.3 Welcome the objectives of the *'Call to Action to end Forced Labour, Modern Slavery and Human Trafficking',* recognizing that legal definitions vary from country to country.

5.4 Uphold and promote the United Nations Convention against Transnational Organized Crime and the Trafficking in Persons Protocol (Palermo Protocol), consistent with national reservations, understandings and declarations.

5.5 Combat trafficking in persons by partnering with the private sector and civil society to counter illicit financial flows stemming from trafficking in persons, including by leveraging financial intelligence and the work by the Financial Action Task Force and its Global Network, as well as investigating and prosecuting.

5.6 Improve information sharing and data exchange within the existing legal framework, explore opportunities for cross-training and draw from best practices and lessons learned from efforts to counterterrorism and efforts to counter transnational organized crime. For example, by continuing to work with the INTERPOL Global Task Force on Human Trafficking.

5.7 Share information and best practices on support for and reintegration of victims.

5.8 Coordinate efforts and share best practices on how to address the use of the internet to facilitate trafficking in persons.

We will also encourage the Roma-Lyon Group on Transnational Organized Crime and Terrorism to:

5.9 Explore the feasibility of a common public messaging campaign.

Source: https://g7.gc.ca/en/g7-presidency/themes/building-peaceful-secure-world/g7-ministerial-meeting/chairs-statement-security-ministers-meeting/g7-security-ministers-commitments-paper/